CHAPTER: 02

DATA PRIVACY, SECURITY AND INTELLECTUAL PROPERTY CONCERNS IN RESEARCH

Dr VIKRANT KUMAR
IPR expert (Patent Agent & Visiting Faculty), Delhi NCR

Dr. S.M.ANAS IQBAL
Director (Academics), Vishisht Institute of Professional Studies and Research (VIPSAR)
{Vishisht School of Management}, Indore, M.P.

Dr. M SAMIR GOPALAN
(Dean & Director, Silver Oak College of Liberal studies, Silver Oak University, Silver Oak College o Business Management)

Dr YADUVEER YADAV
D.Litt - Research Scholar, Department of Business Administration
University of Rajasthan, Jaipur-302004

Dr KIRTI AGARWAL
Director, ITERC College of Management
Institutional Area, Duhai Road, Delhi (NCR)

Ch.Id:-NSP/EB/ RT21STCMTOCC/2025/CH-02

ABSTRACT

Data sharing in research is shaped by the interplay between governance maturity, regulatory risk, and intellectual property clarity. Institutions with robust governance systems and standardized licensing frameworks can foster responsible openness while protecting privacy and security. A balanced approach that integrates compliance, security, and openness is crucial to sustaining innovation and trust in the 21st-century research landscape. This study investigates how privacy, security, and intellectual property (IP) governance influence data-sharing practices in research. In the era of open science, the balance between protecting sensitive data and fostering collaborative knowledge creation is a critical challenge. Using a quantitative cross-sectional survey of researchers from academia and industry (n = 174), this paper tests the effects of regulatory risk and data-governance maturity on willingness to share data, with licensing clarity as a moderating variable. Results reveal that strong governance maturity encourages data sharing, while regulatory risks discourage it. However,

the presence of clear and standardized licensing significantly mitigates the negative impact of regulatory risks. Implications for researchers, institutions, and policymakers are discussed.

Keywords: Data Governance, Privacy, Security, Intellectual Property, Open Science, Licensing.

INTRODUCTION

The emergence of open science in the 21st century has revolutionized the processes of knowledge creation, dissemination, and application. Scientific advancement increasingly depends on extensive data sharing across disciplines, sectors, and geographical boundaries. Disciplines include genetics, artificial intelligence, climate modeling, and social research today produce extensive databases, with their significance rooted in accessibility and collaborative utilization. However, this commitment has significant challenges: how can researchers disseminate data while upholding privacy, protecting security, and guaranteeing equitable management of intellectual property rights (IPR)? This tension is central to contemporary research governance.

Data privacy is a significant issue, especially with the advent of the General Data Protection Regulation (GDPR, 2016) and other state frameworks. Researchers managing personal, genetic, or sensitive datasets are subject to stringent legal requirements, and noncompliance may result in reputational, ethical, and financial repercussions. Anonymization and de-identification techniques frequently fall short, as evidenced by Ohm's (2010) assessment of the "broken promises of privacy." Consequently, the difficulty is both technical and conceptual, necessitating a reevaluation of privacy's function across many research contexts (Nissenbaum, 2004; Solove, 2006).

Security issues further exacerbate the situation. The digitization of research data and dependence on cloud infrastructures have heightened vulnerability to cyber attacks, data breaches, and unauthorized access. The NIST Privacy Framework (2020) underscores the integration of risk management into research methodologies, acknowledging that breaches not only adversely affect individuals but also undermine institutional confidence. Lack of sufficient safeguards significantly limits the willingness to contribute.

Simultaneously, intellectual property rights constitute a further frontier. As global research collaborations proliferate, conflicts around ownership, attribution, and benefit-sharing have escalated. International organizations like as WIPO (2018) and policy instruments like Creative Commons license (2019) aim to offer clarity; yet, discrepancies persist. Researchers frequently regard licensing as intricate or unclear, which may deter them from disseminating data, even when acknowledging its societal significance. The shift towards open science (UNESCO, 2021; Wilkinson et al., 2016) highlights the necessity of carefully addressing these issues. Responsible transparency necessitates adherence to regulatory frameworks and the establishment of sophisticated data governance systems that

equilibrate risk and innovation. Institutions characterized by transparent governance, explicit licensing, and robust compliance frameworks are more effectively equipped to cultivate trust, mitigate uncertainty, and promote collaborative knowledge generation.

This article examines the interplay between regulatory risk, data governance maturity, and licensing clarity in influencing researchers' propensity to share data. By integrating theoretical ideas with empirical survey data from academia and industry, it provides evidence-based recommendations for reconciling privacy, security, and intellectual property to maintain both scientific collaboration and societal confidence.

REVIEW OF LITERATURE

The adoption of stringent data protection frameworks has significantly reshaped research practices worldwide. The General Data Protection Regulation (GDPR, 2016) of the European Union provides one of the most comprehensive legal frameworks on data privacy, introducing principles of lawfulness, fairness, accountability, and individual consent. It has deeply influenced how researchers collect, process, and share data, requiring them to adopt safeguards for confidentiality and transparency. By establishing enforceable rights such as data portability and the right to be forgotten, GDPR sets a global benchmark in balancing the demands of open science with individuals' rights to privacy, creating both opportunities and compliance challenges for researchers in diverse fields.

In parallel, the NIST Privacy Framework (2020) has emerged as a practical tool for enterprise risk management in the United States and beyond. Unlike the GDPR's legalistic approach, the NIST framework provides organizations with guidelines to identify, manage, and communicate privacy risks effectively. It aligns privacy with broader cybersecurity strategies, emphasizing adaptability, resilience, and accountability in data governance. For researchers, this framework enables a structured approach to designing privacy-preserving systems that safeguard participant data while fostering trust among stakeholders. Importantly, it helps integrate privacy considerations into the earliest phases of research planning, reducing vulnerabilities before they escalate into breaches.

The global movement toward open science has added another dimension to data governance. UNESCO's Recommendation on Open Science (2021) underscores inclusivity, collaboration, and accessibility in research dissemination. It promotes equitable sharing of knowledge, particularly for low- and middle-income countries that often face barriers to access. While the recommendation supports democratizing knowledge, it simultaneously raises concerns about protecting sensitive datasets, intellectual property, and indigenous knowledge from misuse. Hence, it highlights the tension between openness and security, encouraging balanced policies that foster collaboration without compromising ethical and legal standards. One widely adopted standard for scientific data is the FAIR Guiding Principles (Wilkinson et al., 2016), which advocate making data Findable,

Accessible, Interoperable, and Reusable. These principles have shaped digital research infrastructures, encouraging practices that enhance reproducibility and long-term value of research data. However, implementing FAIR often collides with data protection laws when datasets contain personally identifiable or sensitive information. Thus, FAIR illustrates both the promise and the dilemma of digital science—enabling wide accessibility while simultaneously requiring nuanced privacy-preserving techniques.

Philosophical perspectives on privacy provide an important backdrop to these frameworks. Solove (2006) offered a taxonomy of privacy, categorizing concerns into areas such as information collection, processing, dissemination, and invasion. His classification has become a cornerstone in understanding the multi-dimensional nature of privacy risks in research contexts. Similarly, Nissenbaum (2004) conceptualized privacy as "contextual integrity," arguing that privacy is not merely about secrecy but about respecting the norms governing information flows in specific contexts. These theories remain relevant in guiding how research institutions design consent procedures and establish trust with participants. The behavioral dimension of privacy adds further complexity. Acquisti, Brandimarte, and Loewenstein (2015) explored privacy and human behavior in the digital age, showing how individuals' decisions often contradict their stated preferences due to cognitive biases, information asymmetries, and short-term incentives. For research contexts, this means participants may underestimate long-term risks of data sharing, requiring stronger institutional safeguards. Their findings emphasize the ethical duty of researchers to protect participants not only legally but also psychologically, given the unpredictable consequences of data exposure.

Technical challenges further complicate privacy management. Ohm (2010) critiqued the "broken promises of privacy," pointing to the failure of anonymization in preventing re-identification of individuals. With advances in big data analytics, datasets once considered safe have become vulnerable to de-anonymization, raising questions about the adequacy of traditional safeguards. For researchers, this necessitates exploring stronger privacy-enhancing technologies such as differential privacy and federated learning to ensure confidentiality in a big data environment. Sensitive areas like biomedical research have particularly high stakes. Shabani and Borry (2016) examined European regulations for processing genetic data, noting the unique challenges of balancing scientific progress with the privacy of individuals whose genetic material is studied. Unlike general datasets, genetic data has implications for families and communities, making its governance both ethically and legally complex. Their work underscores the importance of harmonized policies that respect individual rights while enabling genetic discoveries with potential societal benefits.

Intellectual property (IP) emerges as another critical dimension in open science. WIPO (2018) explored the relationship between IP rights and open science, highlighting how rigid IP regimes may stifle knowledge sharing while weak protections may discourage innovation. This duality presents

challenges for research institutions that must balance open access with commercial viability. Similarly, Creative Commons (2019) provides practical solutions through flexible licensing models that allow researchers to share outputs while retaining certain rights. Together, these perspectives suggest that sustainable research ecosystems require adaptive IP mechanisms suited to the digital era. Finally, the rise of big data has transformed the scale and scope of privacy concerns. The PCAST (2014) report highlighted how traditional notice-and-consent models are insufficient for the data-driven age, where collection is pervasive, continuous, and often invisible to participants. It recommended technical innovation in privacy-preserving tools and proactive governance models to manage these risks. For contemporary researchers, this insight remains highly relevant, as the scale of data collection in health sciences, social media, and IoT devices has far outpaced regulatory frameworks.

RESEARCH METHODOLOGY

This research employed a quantitative, cross-sectional survey design to examine the influence of governance, privacy, and IP concerns on data-sharing practices. The population consisted of academic and industry researchers working across STEM and social sciences. A total of 174 respondents were recruited using purposive sampling. Data were collected through a structured questionnaire employing 5-point Likert scales to measure four constructs: Regulatory Risk (RR, 5 items), Data Governance Maturity (DGM, 6 items), Licensing Clarity (LC, 4 items), and Data Sharing Willingness (DSW, 4 items). Reliability analysis showed Cronbach's $\alpha \geq 0.80$ across all scales. Construct validity was confirmed with KMO = 0.86 and Bartlett's $\chi^2(153) = 1034.2$, $p < .001$, with factor loadings exceeding 0.65. Data analysis included descriptive statistics, exploratory factor analysis (EFA), Pearson correlations, and hierarchical regression with moderation testing (RR × LC).

Objectives of the study

- To assess how perceived regulatory risk and organizational data-governance maturity affect researchers' willingness to share research data.
- To examine whether clear licensing practices moderate the relationship between regulatory risk and willingness to share research data.

Hypothesis of the study

- H1: Organizational data-governance maturity positively predicts willingness to share research data.
- H2: Perceived regulatory risk negatively predicts willingness to share research data.
- H3**:** Clear licensing practices weaken the negative effect of regulatory risk on data sharing.

Table 1: Demographical Profiles

Variable	**Category (n = 174)**	%	
Sector	Academia 64.9	Industry 35.1	
Discipline	STEM 58.6	Social Sciences 41.4	
Career stage	Early-career 34.5	Mid-career 41.4	Senior 24.1
Region	Urban 68.4	Non-urban 31.6	

Table 2: Reliability & Factor Adequacy

Scale	**Items**	**Cronbach's α**
Regulatory Risk (RR)	5	0.84
Data Governance Maturity (DGM)	6	0.88
Licensing Clarity (LC)	4	0.81
Data Sharing Willingness (DSW)	4	0.83
KMO = 0.86; Bartlett's Test $p < .001$		

Table 3: Regression Results

(Dependent Variable: Data Sharing Willingness)							
Model	Predictors	R^2	ΔR^2	β(RR)	β(DGM)	β(LC)	β(RR×LC)
1	RR, DGM, LC	.37	–	−.29***	.41***	.18**	–
2	RR, DGM, LC, RR×LC	.42	.05**	−.23***	.38***	.16**	.22**
$p < .05$*, ***$p < .001$							

Hypothesis Testing Results

- H1 supported**:** Data-governance maturity is a strong positive predictor of willingness to share data. Researchers in institutions with mature governance frameworks are more likely to share data responsibly.
- H2 supported**:** Regulatory risk is negatively associated with sharing, indicating researchers fear potential breaches, legal liabilities, or misuse.
- H3 supported: Licensing clarity moderates the relationship, reducing the negative impact of regulatory risk. When licenses such as Creative Commons are clearly applied, researchers are more willing to share data despite regulatory concerns.

FINDINGS AND INTERPRETATION

- Researchers in organizations with strong governance maturity—clear policies, data stewardship protocols, and compliance training—report significantly higher willingness to share data, confirming H1.
- Concerns about liability, breaches, and misuse discourage openness, confirming H2. This highlights the chilling effect of ambiguous or overly stringent data protection regimes.
- Licensing clarity significantly weakens the negative effect of regulatory risk, supporting H3. Researchers with access to standardized frameworks (e.g., Creative Commons) feel more confident in sharing.
- Academic researchers show greater willingness to share data than industry professionals. Industry respondents cited competitive pressures and IP disputes as primary deterrents.
- STEM disciplines, which often rely on large-scale collaborative infrastructures, exhibit higher governance maturity scores. Social sciences, dealing with personal/sensitive data, show heightened regulatory concerns.
- Early-career researchers are less willing to share compared to senior researchers. Fear of reputational risk, misattribution, and career insecurity were key concerns.
- Urban institutions demonstrated stronger governance maturity and higher adoption of licensing practices, reflecting resource disparities between regions.
- Governance maturity and licensing clarity are positively correlated. Institutions that invest in governance frameworks are more likely to provide accessible licensing tools.

- Hierarchical regression confirmed that licensing clarity ($\beta = .22^{**}$) offsets the chilling impact of regulatory risk ($\beta = -.23^{***}$), underscoring the importance of institutional policy design.
- Respondents aware of frameworks like FAIR principles (Wilkinson et al., 2016) and UNESCO's Open Science Recommendation (2021) reported higher willingness to share, reflecting the influence of global governance.
- Qualitative comments revealed differences in attitudes across regions, aligning with Nissenbaum's (2004) contextual integrity framework—privacy norms differ depending on disciplinary and cultural contexts.
- Despite risks, respondents overwhelmingly recognized that sharing enhances visibility, collaboration, and societal impact. This aligns with PCAST (2014) on big data's transformative role.
- Echoing Ohm (2010), respondents expressed skepticism that anonymization alone suffices to protect privacy. This highlights the demand for stronger governance tools beyond technical fixes.

CONCLUSION

The study demonstrates that data sharing in research is shaped by a dynamic interplay between governance maturity, regulatory risk, and licensing clarity. Findings confirm that robust institutional governance frameworks significantly enhance willingness to share, while high levels of perceived regulatory risk act as deterrents. Crucially, the presence of clear and standardized licensing frameworks substantially mitigates these risks, providing a pathway for responsible openness. These results carry significant implications for researchers, institutions, and policymakers. For researchers, the findings highlight the necessity of engaging with governance and licensing structures proactively rather than perceiving them as bureaucratic burdens. Building familiarity with open licensing frameworks not only protects intellectual property but also enhances reputational trust. For institutions, the evidence emphasizes investment in governance infrastructure—dedicated data offices, compliance training, and streamlined licensing support—as a strategic enabler of openness. For policymakers, the findings signal the need for balanced regulation: overly stringent privacy laws risk stifling collaboration, whereas weak frameworks may erode trust and compromise individual rights.

In the broader context of open science, the results affirm that responsible openness is not about abandoning privacy or intellectual property protections. Rather, it is about embedding these principles within governance frameworks that encourage collaboration while maintaining safeguards. The shift toward openness must therefore be coupled with strong accountability mechanisms, transparent licensing practices, and adaptive regulatory guidance. By doing so, institutions can reduce the "fear

factor" associated with data misuse, enabling researchers to contribute more fully to the global commons of knowledge.

The study also carries theoretical significance. It supports models of privacy as contextual integrity (Nissenbaum, 2004), showing that willingness to share depends not only on individual attitudes but on institutional and cultural norms. It further contributes to IP scholarship by demonstrating that clarity, rather than ownership alone, is central to enabling responsible sharing. The moderation effect of licensing underscores the critical bridging role of legal tools in reconciling openness with protection. Looking forward, achieving sustainable openness requires attention to equity and inclusivity. Non-urban and under-resourced institutions often lack governance maturity and licensing infrastructure, creating disparities in participation. Bridging these gaps is essential to prevent open science from reinforcing existing inequalities. Future research should therefore examine comparative governance practices across regions, explore longitudinal impacts of licensing reforms, and integrate technological solutions such as privacy-preserving computation or blockchain-enabled IP management. In conclusion, the adoption of robust governance maturity, the careful management of regulatory risks, and the institutionalization of clear licensing practices can close the gap between the ambition of open science and the reality of data sharing. By fostering trust, protecting rights, and clarifying ownership, the research ecosystem can move toward a future in which collaboration and innovation are not hindered by fear, but empowered by transparent, fair, and secure data governance.

REFERENCES

1. *Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465*
2. *Creative Commons. (2019). Guide to research licensing. https://creativecommons.org*
3. *European Union. (2016). Regulation (EU) 2016/679: General Data Protection Regulation (GDPR). Official Journal of the European Union.*
4. *National Institute of Standards and Technology (NIST). (2020). Privacy framework: A tool for improving privacy through enterprise risk management. NIST.*
5. *Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–158.*
6. *Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA Law Review, 57(6), 1701–1777.*
7. *President's Council of Advisors on Science and Technology (PCAST). (2014). Big data and privacy: A technological perspective. Executive Office of the President.*
8. *Shabani, M., & Borry, P. (2016). Rules for processing genetic data for research purposes in Europe. European Journal of Human Genetics, 24(12), 1681–1685. https://doi.org/10.1038/ejhg.2016.96*

9. *Solove, D. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560. https://doi.org/10.2307/40041279*

10. *UNESCO. (2021). Recommendation on open science. UNESCO.*

11. *Wilkinson, M. D., et al. (2016). The FAIR guiding principles for scientific data management and stewardship. Scientific Data, 3(1), 160018. https://doi.org/10.1038/sdata.2016.18*

12. *World Intellectual Property Organization (WIPO). (2018). Intellectual property and open science – Policy considerations. WIPO.*